

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001年9月20日 (20.09.2001)

PCT

(10) 国際公開番号  
WO 01/69842 A1

- (51) 国際特許分類7: H04L 9/08, 9/10, 9/32
- (21) 国際出願番号: PCT/JP01/02003
- (22) 国際出願日: 2001年3月14日 (14.03.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2000-70672 2000年3月14日 (14.03.2000) JP
- (71) 出願人(米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒100-8220 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).

日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-0052 東京都港区赤坂4丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

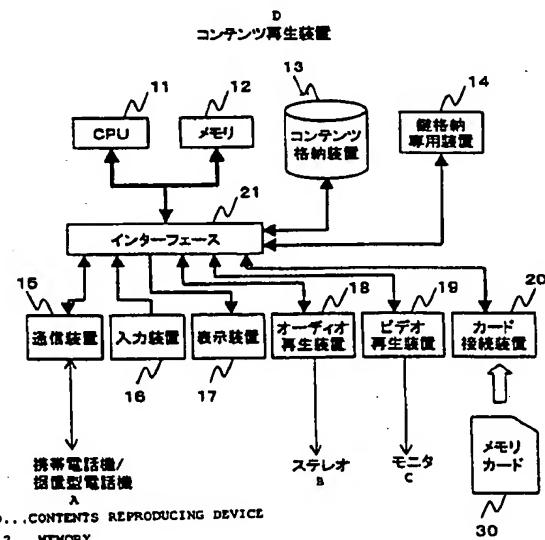
(72) 発明者: および

(75) 発明者/出願人(米国についてのみ): 常広 隆司 (TSUNEHIRO, Takashi) [JP/JP]. 片山 弘 (KATAYAMA, Kunihiro) [JP/JP]. 水島 永雅 (MIZUSHIMA, Nagamasa) [JP/JP]. 真野 宏之 (MANO, Hiroyuki) [JP/JP]; 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社 日立製作所 システム

[統葉有]

(54) Title: CONTENTS REPRODUCING DEVICE

(54) 発明の名称: コンテンツ再生装置



- D...CONTENTS REPRODUCING DEVICE  
12...MEMORY  
13...CONTENTS STORING DEVICE  
14...KEY-ONLY STORING DEVICE  
21...INTERFACE  
15...COMMUNICATION DEVICE  
16...INPUT DEVICE  
17...DISPLAY DEVICE  
18...AUDIO REPRODUCING DEVICE  
19...VIDEO REPRODUCING DEVICE  
20...CARD CONNECTING DEVICE  
A...PORTABLE PHONE/FIXED PHONE  
B...STEREO  
C...MONITOR  
30...MEMORY CARD

(57) Abstract: A license key provided for each element of contents data is stored in a key-only storing device provided separately from a contents storing device; the key-only storing device performs an authentication processing on a communicating partner, and, when authenticated, sends a license key corresponding to contents data to be reproduced to a reproducing device using an encrypted communication, whereby the reproducing device decodes the contents data to be reproduced using the license key and reproduces it.

WO 01/69842 A1

[統葉有]



開発研究所内 Kanagawa (JP). 戸塚 隆 (TOTSUKA, Takashi) [JP/JP]. 中村一男 (NAKAMURA, Kazuo) [JP/JP]; 〒187-0022 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 藤 茂夫 (TODOROKI, Shigeo) [JP/JP]; 〒107-0052 東京都港区赤坂4丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]; 〒503-0116 岐阜県安八郡安八町大森180 三洋電機株式会社内 Gifu (JP). 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

- (74) 代理人: 富田和子(TOMITA, Kazuko); 〒220-0004 神奈川県横浜市西区北幸二丁目9-10 横浜HSビル7階 Kanagawa (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM,

DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:  
— 國際調査報告書

2 文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

---

(57) 要約:

コンテンツデータ毎に用意されたライセンス鍵をコンテンツ格納装置とは別に設けられた鍵格納専用装置に格納し、該鍵格納専用装置は通信相手に認証処理を施し、認証された場合には、暗号通信を利用して再生装置に再生対象コンテンツデータに対応するライセンス鍵を送信することで、前記再生装置は再生対象コンテンツデータを、前記ライセンス鍵を用いて復号して再生する。

## 明細書

## コンテンツ再生装置

## 技術分野

本発明は、正当な権利者のみに、オーディオデータやビデオデータなどのコンテンツデータの再生を許可する技術に関し、特に、大量のコンテンツデータを再生可能な据置型のコンテンツ再生装置に好適な技術に関する。

## 背景技術

近年、オーディオデータやビデオデータなどのコンテンツデータをネットワークを介して配信しようとする試みがなされている。たとえば、専用のメモリカードを用意し、これを販売店などに設置された専用端末に装着し、オンラインシステムを利用して所望のコンテンツデータを前記メモリカード内にダウンロードする。あるいは、専用のメモリカードを携帯電話機等の個人向け端末に装着し、インターネットを利用して、コンテンツ配信センタから前記メモリカード内にダウンロードする。コンテンツデータを再生する場合には、コンテンツデータを格納した前記メモリカードを専用の再生装置に装着し、再生する。

## 発明の開示

さて、上述のような専用のメモリカードと再生装置からなるシステム

において、コンテンツデータは複製が容易であることから、コンテンツデータを格納する専用のメモリカードには、コピー防止機能を設けるなどしてコンテンツ著作者などの保護を図る必要がある。

しかしながら、メモリカードでは、容量に限界があるため、大量のコンテンツデータを保存することができない。ユーザは、現在利用していないコンテンツデータであっても、コレクションとしてとっておきたい場合がある。この場合、メモリカードにコピー防止機能が付加されると、ユーザは、メモリカードがコンテンツデータで満杯になる都度、新たなメモリカードを購入しなければならず、経済的な負担が大きい。

また、ユーザは、コレクションとしてとっておいたコンテンツデータを再生したい場合、数あるメモリカードの中から再生したいコンテンツデータを記憶したメモリカードを見つけ出し、専用の再生装置に装着しなければならない。そして、再生したいコンテンツデータを記憶したメモリカードが変わる都度、再生装置に装着するメモリカードを変更しなければならず手間である。

このような、コピー防止機能が付いたメモリカードと再生装置からなるシステムは、携帯用に適しているが、たとえば、家のなかでコンテンツデータの再生を楽しむような据置型には適していない。

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、コンテンツ著作者などの保護を図りつつも、メモリカードの交換なしに、大量のコンテンツデータを再生できるようにすることにある。

上記課題を解決するために、本発明のコンテンツ再生装置では、コンテンツデータもしくは当該データのグループ毎に異なる鍵で暗号化されたコンテンツデータを再生する。コンテンツデータもしくは当該データのグループ毎に用意された、暗号化されたコンテンツデータを復号するための鍵は、暗号化されたコンテンツデータを格納するコンテンツ格納

手段とは別個に設けられた計算機能付き格納手段に格納しておく。

ここで、計算機能付き鍵格納手段は、通信相手を認証する認証手段を有し、当該認証手段によりコンテンツ再生装置の再生手段が通信相手として認証された場合に、暗号通信を利用して、再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信する。また、再生手段は、コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し再生する。

本発明において、コンテンツ格納手段に格納されたコンテンツデータは暗号化されているので、対応する鍵がなければ復号し再生することができない。したがって、コンテンツ格納手段にコピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納手段として、一般に市販されている大容量のハードディスク装置などを利用できる。このため、大量のコンテンツデータを格納することが可能となる。

また、コンテンツ格納手段に格納されたコンテンツデータを復号するためには対応する鍵が必要となるため、この鍵が計算機能付き鍵格納手段に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者（対応する鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

さらに、本発明では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行う再生手段で行うようにしている。そして、計算機能付き鍵格納手段は、鍵の送信相手が再生手段であることを認証した場合に、当該鍵を暗号通信を利用して前記再生手段に送るようにしている。このようにすることで、鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

なお、一般に、暗号化されたコンテンツデータを復号するための鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、計算機能付き鍵格納手段として、本コンテンツ再生装置に装着自在に構成された、従来の技術で説明したようなコピー防止機能を備えたメモリカードを用いた場合でも、当該メモリカードに大量のコンテンツデータに対応する鍵を格納することができる。したがって、再生するコンテンツを変えるときにメモリカードを差し替えなければならないといった事態が頻繁に生じるのを防ぐことができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

#### 図面の簡単な説明

図1は、本発明の1実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

図2は、図1に示す鍵格納専用装置14の概略構成を示す図である。

図3は、図1に示すオーディオ再生装置18の概略構成を示す図である。

図4は、図1に示すビデオ再生装置19の概略構成を示す図である。

図5は、本発明の1実施形態が適用されたコンテンツ再生装置の概観の一例を示す図である。

図6は、本発明の第1実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。

図7は、図6に示すフローにおける鍵格納専用装置14およびオーディオ再生装置18/ビデオ再生装置19間のデータのやり取りの一例を説明するためのシーケンス図である。

図8は、本発明の第1実施形態が適用されたコンテンツ再生装置に接続されたメモリカード30からライセンス鍵入手する場合の動作を説明するためのフロー図である。

図9は、図8に示すフローにおける鍵格納専用装置14およびメモリカード30間のデータのやり取りの一例を説明するためのシーケンス図である。

図10は、本発明の1実施形態が適用されたコンテンツ再生装置の鍵格納専用装置14から本コンテンツ再生装置に接続されたメモリカード30へライセンス鍵を移動する場合の動作を説明するためのフロー図である。

#### 発明を実施するための最良の形態

以下に、本発明の1実施形態について説明する。

図1は、本発明の1実施形態が適用されたコンテンツ再生装置の概略構成を示す図である。

図1において、CPU11は、本コンテンツ再生装置の各部を統括的に制御する。メモリ12は、ROMおよびRAMから構成される。ROMには、CPU11が本コンテンツ再生装置の各部を統括的に制御するためのプログラムが格納されている。RAMは、CPU11のワークエリアとして機能する。

コンテンツ格納装置13は、たとえばハードディスク装置などの大容量記憶装置で構成されており、暗号化されたオーディオデータやビデオデータなどのコンテンツデータがそのコンテンツ名称に対応付けられて格納される。

鍵格納専用装置14は、コンテンツ毎に用意された、暗号化されたコ

ンテンツデータを復号するための鍵（以下、ライセンス鍵と称する）を格納する。

通信装置 15 は、携帯電話機や据置型の電話機に接続し、オンラインシステムやインターネットなどのネットワークを介して、たとえば暗号化されたコンテンツデータやライセンス鍵を配信するコンテンツ配信センタ（不図示）にアクセスし、暗号化されたコンテンツデータやライセンス鍵入手するのに用いられる。

入力装置 16 は、たとえば各種ボタンやタッチパネルで構成され、ユーザからの再生指示やコンテンツデータ、ライセンス鍵の入手指示を受け付ける。

表示装置 17 は、たとえば液晶パネルで構成され、コンテンツ格納装置 13 に格納されている暗号化されたコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。

オーディオ再生装置 18 は、コンテンツ格納装置 13 のなかから再生対象の暗号化されたオーディオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、オーディオ信号を得る。そして、オーディオ信号を本コンテンツ再生装置に接続されたステレオに出力する。ビデオ再生装置 19 は、コンテンツ格納装置 13 のなかから再生対象の暗号化されたビデオデータを読み出し、これに対応するライセンス鍵を用いて復号し再生して、ビデオ信号を得る。そして、ビデオ信号を本コンテンツ再生装置に接続されたモニタに出力する。

カード接続装置 20 は、メモリカード 30 を接続し、当該メモリカード 30 から暗号化されたコンテンツデータやライセンス鍵入手したり、当該メモリカード 20 へ暗号化されたコンテンツデータやライセンス鍵を送ったりする。

インターフェース 21 は、CPU 11 やメモリ 12 と本コンテンツ再生装置を構成する他装置との間のデータ送受を司る。

次に、本コンテンツ再生装置を構成する各装置のうち、鍵格納専用装置 14、オーディオ再生装置 18 およびビデオ再生装置 19 について、さらに詳細に説明する。

まず、鍵格納専用装置 14 について説明する。

図 2 は、鍵格納専用装置 14 の概略構成を示す図である。

図示するように、鍵格納専用装置 14 は、CPU 141 と、メモリ 142 と、フラッシュメモリ 143 と、インターフェース 21 を介して本コンテンツ再生装置の各部とデータ送受を行うための I/O 回路 144 と、を有する。

CPU 141 は、鍵格納専用装置 14 の各部を統括的に制御する。また、CPU 141 は、認証機能と暗復号化機能を有している。メモリ 142 は、ROM および RAM から構成される。ROM には、CPU 141 が鍵格納専用装置 14 の各部を統括的に制御するためのプログラムと、認証機能および暗復号化機能を実現するためのプログラムが格納されている。RAM は、CPU 141 のワークエリアとして機能する。フラッシュメモリ 143 には、ライセンス鍵が復号対象コンテンツのコンテンツ名称に対応付けられて格納される。ここで、ライセンス鍵は、セキュリティをより強固にするため、いわゆるタンパ・レジスタント領域 (TRM: Tamper Resistant Module) に格納するのがよい。なお、フラッシュメモリ 143 の代わりに、FRAM や EEPROM などのその他の不揮発性メモリを用いることができる。

図 2 に示す鍵格納専用装置 14 を構成する各部は、たとえば 1 チップ上につくり込まれるようにしてもよいし、あるいは、複数チップで構成されるようにしてもよい。複数チップで構成する場合は、鍵格納専用装

置 1 4 の外部からチップ間の信号を盗み取られないような工夫を施すことが好ましい。

次に、オーディオ再生装置 1 8 について説明する。

図 3 は、オーディオ再生装置 1 8 の概略構成を示す図である。

図示するように、オーディオ再生装置 1 8 は、暗復号化回路 1 8 1 と、デコーダ回路 1 8 2 と、インターフェース 2 1 を介して本コンテンツ再生装置の各部とデータ送受を行うための I/O 回路 1 8 4 と、を有する。

暗復号化回路 1 8 1 は、鍵格納専用装置 1 4 から再生対象の暗号化されたオーディオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置 1 3 から読み出された再生対象の暗号化されたオーディオデータを復号する。デコーダ回路 1 8 2 は、暗復号化回路 1 8 1 で復号化されたオーディオデータを、必要に応じて伸長し、再生して、オーディオ信号を得る。そして、オーディオ信号をステレオに出力する。

次に、ビデオ再生装置 1 9 について説明する。

図 4 は、ビデオ再生装置 1 9 の概略構成を示す図である。

図示するように、ビデオ再生装置 1 9 は、暗復号化回路 1 9 1 と、デコーダ回路 1 9 2 と、フレームバッファ 1 9 3 と、インターフェース 2 1 を介して本コンテンツ再生装置の各部とデータ送受を行うための I/O 回路 1 9 4 とを有する。

暗復号化回路 1 9 1 は、鍵格納専用装置 1 4 から再生対象の暗号化されたビデオデータに対応するライセンス鍵を入手し、この鍵を用いて、コンテンツ格納装置 1 3 から読み出された再生対象の暗号化されたビデオデータを復号する。デコーダ回路 1 9 2 は、フレームバッファ 1 9 3 を利用して、暗復号化回路 1 9 1 で復号化されたビデオデータを、必要に応じて伸長し、再生して、ビデオ信号を得る。そして、ビデオ信号を

モニタに出力する。

次に、本コンテンツ再生装置に装着されて用いられるメモリカード30について説明する。

メモリカード30の概略構成は、図2に示す鍵格納専用装置14と同じである。ただし、メモリカード30には、ライセンス鍵のみならず、暗号化されたコンテンツデータも格納されるものとする。すなわち、このメモリカード30は、たとえば販売店などに設置された専用端末に装着されて、ユーザがオンラインシステムを利用して所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したり、あるいは、携帯電話機等の個人向け端末に装着されて、ユーザがインターネットを利用してコンテンツ配信センタから所望の暗号化されたコンテンツデータやそのライセンス鍵を入手したりするのに用いることができるものとする。

ここで、図5に、本実施形態が適用されたコンテンツ再生装置の概観の一例を示す。図示するように、本コンテンツ再生装置は、家庭内でコンテンツを楽しむのに適した据置型の形状をしている。ここで、符号41は、再生ボタン、停止ボタン、再生コンテンツ選択ボタン、および、コンテンツデータやライセンス鍵をコンテンツ格納装置13や鍵格納専用装置14へ書き込んだり、カード接続装置30に接続されたメモリカード20へ移動したりするための各種設定ボタンなどで構成される操作パネルである。符号42は、操作パネル41と同じ各種ボタンを備えたリモコン50からの指示を受け付けるための受信部である。符号43は、表示パネルであり、コンテンツ格納装置13に格納されているコンテンツデータのコンテンツ名称のリストを表示したり、再生対象の暗号化されたコンテンツデータのコンテンツ名称を表示したりする。そして、符号44は、メモリカード30を装着するためのスロットである。なお、図示していないが、本コンテンツ装置の背面には、モニタ51やステレ

オ 5 2 や携帯電話機 5 3 あるいは電話機を接続するための端子が設けられている。

次に、本実施形態のコンテンツ再生装置の動作について説明する。

まず、コンテンツデータを再生する場合の動作について説明する。

図 6 は、本実施形態が適用されたコンテンツ再生装置の再生動作を説明するためのフロー図である。このフローは、たとえば、ユーザが入力装置 1 6 を用いて、表示装置 1 7 に表示された、コンテンツ格納装置 1 3 に格納されているコンテンツデータのコンテンツ名称のリストの中から、再生対象のコンテンツを選択し、再生指示を入力すると開始される。

まず、C P U 1 1 は、入力装置 1 6 を介してユーザより受け付けたコンテンツデータの再生指示を、当該コンテンツデータの種類（オーディオデータ/ビデオデータ）を再生するオーディオ再生装置 1 8 /ビデオ再生装置 1 9 に送信する（S 1 0 0 1）。

C P U 1 1 より再生指示を受け取ったオーディオ再生装置 1 8 /ビデオ再生装置 1 9 の暗複号化回路 1 8 1 /1 9 1 は、自身の認証データと再生対象の暗号化されたコンテンツデータの識別情報（たとえばコンテンツ名称）を含んだ、当該コンテンツデータ再生のためのライセンス鍵送信指示を、鍵格納専用装置 1 4 に送信する（S 1 0 0 2）。

鍵格納専用装置 1 4 の C P U 1 4 1 は、コンテンツデータ再生のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う（S 1 0 0 3）。たとえば、認証データが予め本鍵格納専用装置 1 4 に登録されているオーディオ/ビデオ再生装置であることを示しているか否かを調べる。そして、当該指示の送信元がオーディオ再生装置 1 8 /ビデオ再生装置 1 9 であることを認証したならば（S 1 0 0 4 で Y e s の場合）、当該指示に含まれる識別情報によ

り特定されるコンテンツデータのライセンス鍵がフラッシュメモリ 143 に格納されているか否かを調べる (S1005)。格納されていれば (S1006 で Yes の場合)、そのライセンス鍵をフラッシュメモリ 143 から読み出し、暗号通信を利用して、当該指示の送信元であるオーディオ再生装置 18 / ビデオ再生装置 19 に送信する (S1008)。

なお、S1004において指示の送信元がオーディオ再生装置 18 / ビデオ再生装置 19 であることを認証できなかった場合、および、S1006において所望のライセンス鍵がフラッシュメモリ 143 に格納されていなかった場合、鍵格納専用装置 14 の CPU141 は、CPU11 にその旨伝える。これを受けて、CPU11 は表示装置 17 にエラー表示を行うなど、所定のエラー処理を行う (S1007)。

さて、コンテンツデータ再生のためのライセンス鍵送信指示を送信したオーディオ再生装置 18 / ビデオ再生装置 19 の暗複号化回路 181 / 191 は、鍵格納専用装置 14 からライセンス鍵を受け取ると、コンテンツ格納装置 13 から再生対象の暗号化されたコンテンツデータを読み出す (S1009)。そして、これをライセンス鍵で復号して、デコーダ回路 182 / 192 に渡す。デコーダ回路 182 / 192 は、暗復号化回路 181 / 191 から受け取ったコンテンツデータを必要に応じて伸長し、再生してオーディオ / ビデオデータを得、ステレオ / モニタに出力する (S1010)。

次に、図 6 に示すフローにおける鍵格納専用装置 14 およびオーディオ再生装置 18 / ビデオ再生装置 19 間のデータのやり取りについて、その一例を説明する。

図 7 は、図 6 に示すフローにおける鍵格納専用装置 14 およびオーディオ再生装置 18 / ビデオ再生装置 19 間のデータのやり取りの一例を説明するためのシーケンス図である。

オーディオ再生装置18/ビデオ再生装置19の暗復号化回路181/191は、図6のS1002において、自身の認証データと、再生対象の暗号化されたコンテンツデータの識別情報と、予め保持しているメディアクラス秘密鍵 $K_{PHC}$ と対のメディアクラス公開鍵 $K_{OMC}$ とを含んだライセンス鍵送信指示を作成し、これを鍵格納専用装置14に送信する(T1001)。

これを受け、鍵格納専用装置14のCPU141は、図6のS1004～S1007において、オーディオ再生装置18/ビデオ再生装置19の認証、および、フラッシュメモリ143に要求されたライセンス鍵が格納されていることの確認を行う(T1002)。それから、CPU141は、セッション鍵 $K_{s1}$ を生成し(T1003)、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵 $K_{OMC}$ で暗号化して、当該指示の送信元であるオーディオ再生装置18/ビデオ再生装置19に送信する(T1004)。

これを受け、オーディオ再生装置18/ビデオ再生装置19の暗復号化回路181/191は、暗号化されたセッション鍵 $K_{s1}$ を予め保持しているメディアクラス秘密鍵 $K_{PHC}$ で復号し、セッション鍵 $K_{s1}$ を得る(T1005)。それから、乱数 $K_{s2}$ を生成し(T1006)、セッション鍵 $K_{s1}$ で暗号化して、鍵格納専用装置14に送信する(T1007)。

これを受け、鍵格納専用装置14のCPU141は、暗号化された乱数 $K_{s2}$ を、セッション鍵 $K_{s1}$ で復号し、乱数 $K_{s2}$ を得る(T1008)。そして、送信を要求されているライセンス鍵 $K_c$ を乱数 $K_{s2}$ で暗号化して、ライセンス鍵送信指示の送信元であるオーディオ再生装置18/ビデオ再生装置19に送信する(T1009)。

これを受け、オーディオ再生装置18/ビデオ再生装置19の暗複

号化回路 181 / 191 は、暗号化されたライセンス鍵  $K_c$  を乱数  $K_{s2}$  を用いて復号し、ライセンス鍵  $K_c$  を得る (T1010)。

以上、コンテンツデータを再生する場合の動作について説明した。

次に、メモリカード 30 からライセンス鍵入手する場合の動作について説明する。

図 8 は、本実施形態が適用されたコンテンツ再生装置に接続されたメモリカード 30 からライセンス鍵入手する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード 30 が装着された状態で、ユーザが入力装置 16 を用いて、表示装置 17 に表示された、メモリカード 30 に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、入手対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵入手指示を入力すると開始される。

まず、CPU11 は、入力装置 16 を介してユーザよりライセンス鍵入手指示を受け付けたならば、その旨を鍵格納専用装置 14 に送信する (S2001)。

CPU11 よりライセンス鍵入手指示を受け取った鍵格納専用装置 14 の CPU141 は、自身の認証データと入手対象のライセンス鍵の識別情報（たとえば当該鍵で復号可能なコンテンツの名称）を含んだ、当該ライセンス鍵入手のためのライセンス鍵送信指示を、カード接続装置 20 に接続されたメモリカード 30 に送信する (S2002)。

メモリカード 30 の CPU は、ライセンス鍵入手のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う (S2003)。たとえば、認証データが予め本メモリカード 30 に登録されている鍵格納専用装置であることを示しているか否かを調べる。そして、当該指示の送信元が鍵格納専用装置 14 であるこ

とを認証したならば（S 2 0 0 4でY e sの場合）、当該指示に含まれる識別情報により特定されるライセンス鍵がメモリカード3 0内に格納されているか否かを調べる（S 2 0 0 5）。格納されていれば（S 2 0 0 6でY e sの場合）、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元である鍵格納専用装置1 4に送信する（S 2 0 0 8）。それから、送信したライセンス鍵をメモリカード3 0内から消去する（S 2 0 0 9）。

なお、S 2 0 0 4において指示の送信元が鍵格納専用装置1 4であることを認証できなかった場合、および、S 2 0 0 6において所望のライセンス鍵がメモリカード3 0内に格納されていなかった場合、メモリカード3 0のC P Uは、C P U 1 1にその旨伝える。これを受け、C P U 1 1は表示装置1 7にエラー表示を行うなど、所定のエラー処理を行う（S 2 0 0 7）。

さて、ライセンス鍵入手のためのライセンス鍵送信指示を送信した鍵格納専用装置1 4のC P U 1 4 1は、カード接続装置2 0に接続されたメモリカード3 0からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてフラッシュメモリ1 4 3に格納する（S 2 0 1 0）。

次に、図8に示すフローにおける鍵格納専用装置1 4およびメモリカード3 0間のデータのやり取りについて、その一例を説明する。

図9は、図8に示すフローにおける鍵格納専用装置1 4およびメモリカード3 0間のデータのやり取りの一例を説明するためのシーケンス図である。

鍵格納専用装置1 4のC P U 1 4 1は、図8のS 2 0 0 2において、自身の認証データと、入手対象のライセンス鍵の識別情報と、予め保持しているメディアクラス秘密鍵K' <sub>P M C</sub>と対のメディアクラス公開鍵K' <sub>D</sub>

<sub>MC</sub>とを含んだライセンス鍵送信指示を作成し、これをメモリカード30に送信する（T2001）。

これを受け、メモリカード30のCPUは、図8のS2004～S2007において、鍵格納専用装置14の認証、および、メモリカード30内に要求されたライセンス鍵が格納されていることの確認を行う（T2002）。それから、メモリカード30のCPUは、セッション鍵K<sub>s1</sub>を生成し（T2003）、これをライセンス鍵送信指示に含まれているメディアクラス公開鍵K'<sub>0MC</sub>で暗号化して、当該指示の送信元である鍵格納専用装置14に送信する（T2004）。

これを受け、鍵格納専用装置14のCPU141は、暗号化されたセッション鍵K<sub>s1</sub>を予め保持しているメディアクラス秘密鍵K'<sub>PMC</sub>で復号し、セッション鍵K<sub>s1</sub>を得る（T2005）。それから、乱数K<sub>s2</sub>を生成し（T2006）、これと、予め保持しているメディア固有秘密鍵K'<sub>PM</sub>と対のメディア固有公開鍵K'<sub>0M</sub>とを、セッション鍵K<sub>s1</sub>で暗号化して、メモリカード30に送信する（T2007）。

これを受け、メモリカード30のCPUは、暗号化された乱数K<sub>s2</sub>とメディア固有公開鍵K'<sub>0M</sub>を、セッション鍵K<sub>s1</sub>で復号し、乱数K<sub>s2</sub>とメディア固有公開鍵K'<sub>0M</sub>を得る（T2008）。そして、送信を要求されているライセンス鍵K<sub>c</sub>をメディア固有公開鍵K'<sub>0MC</sub>で暗号化し、さらにこれを乱数K'<sub>s2</sub>で暗号化して、ライセンス鍵送信指示の送信元である鍵格納専用装置14に送信する（T2009）。

これを受け、鍵格納専用装置14のCPU141は、暗号化されたライセンス鍵K<sub>c</sub>を乱数K<sub>s2</sub>とメディア固有秘密鍵K'<sub>PM</sub>を用いて復号し、ライセンス鍵K<sub>c</sub>を得る（T2010）。

以上、メモリカード30からライセンス鍵入手する場合の動作について説明した。

次に、本コンテンツ再生装置の鍵格納専用装置14に格納されているライセンス鍵をメモリカード30へ移動する場合の動作について説明する。

図10は、本実施形態が適用されたコンテンツ再生装置の鍵格納専用装置14から本コンテンツ再生装置に接続されたメモリカード30へライセンス鍵を移動する場合の動作を説明するためのフロー図である。このフローは、たとえば、本コンテンツ再生装置にメモリカード30が装着された状態で、ユーザが入力装置16を用いて、表示装置17に表示された、鍵格納専用装置14に格納されているライセンス鍵に対応するコンテンツ名称のリストのなかから、移動対象のライセンス鍵に対応するコンテンツを選択し、ライセンス鍵移動指示を入力すると開始される。

まず、CPU11は、入力装置16を介してユーザよりライセンス鍵移動指示を受け付けたならば、その旨をメモリカード30に送信する(S3001)。

CPU11よりライセンス鍵移動指示を受け取ったメモリカード30のCPUは、自身の認証データと移動対象のライセンス鍵の識別情報(たとえば当該鍵で復号可能なコンテンツの名称)を含んだ、当該ライセンス鍵移動のためのライセンス鍵送信指示を、鍵格納専用装置14に送信する(S3002)。

鍵格納専用装置14のCPU141は、ライセンス鍵移動のためのライセンス鍵送信指示を受け取ったならば、当該指示に含まれる認証データを用いて検証を行う(S3003)。たとえば、認証データが予め本鍵格納専用装置14に登録されているメモリカード30であることを示しているか否かを調べる。そして、当該指示の送信元がメモリカード30であることを認証したならば(S3004でYesの場合)、当該指示に含まれる識別情報により特定されるライセンス鍵がフラッシュメモ

リ 1 4 3 内に格納されているか否かを調べる (S 3 0 0 5)。格納されていれば (S 3 0 0 6 で Yes の場合)、そのライセンス鍵を読み出し、暗号通信を利用して、当該指示の送信元であるメモリカード 3 0 に送信する (S 3 0 0 8)。それから、送信したライセンス鍵をフラッシュメモリ 1 4 3 内から消去する (S 3 0 0 9)。

なお、S 3 0 0 4 において指示の送信元がメモリカード 3 0 であることを認証できなかった場合、および、S 3 0 0 6 において所望のライセンス鍵がフラッシュメモリ 1 4 3 内に格納されていなかった場合、鍵格納専用装置 1 4 の C P U 1 4 1 は、C P U 1 1 にその旨伝える。これを受けて、C P U 1 1 は表示装置 1 7 にエラー表示を行うなど、所定のエラー処理を行う (S 3 0 0 7)。

さて、ライセンス鍵移動のためのライセンス鍵送信指示を送信したメモリカード 3 0 の C P U は、鍵格納専用装置 1 4 からライセンス鍵を受け取ると、これをたとえば当該鍵で復号可能なコンテンツデータのコンテンツ名称に対応付けてメモリカード 3 0 内に格納する (S 3 0 1 0)。

なお、図 1 0 に示すフローにおける鍵格納専用装置 1 4 およびメモリカード 3 0 間のデータのやり取りは、図 9 に示すシーケンス図において、鍵格納専用装置 1 4 およびメモリカード 3 0 の動作を互いに交換したものとなる。

以上、メモリカード 3 0 へライセンス鍵を移動する場合の動作について説明した。

なお、通信装置 1 5 に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）からライセンス鍵入手する場合の動作は、一般的な、ネットワークを介したデータダウンロードと同じものでよい。ただし、正当な権利を有する者のみがライセンス鍵入手でき

るようにするために、鍵格納専用装置 14 とコンテンツ配信センタとの間で認証処理を行い、コンテンツ配信センタが鍵格納専用装置 14 を認証した場合にのみ、ライセンス鍵のダウンロードを許可するようにすることが好ましい。また、コンテンツデータのコンテンツ格納装置 13 へのダウンロードは、たとえば、メモリカード 30 に格納されたコンテンツデータをコピーしてコンテンツ格納装置 13 に格納するようにしてよいし、あるいは、通信装置 15 に接続された携帯電話機/据置型電話機を利用して、オンラインシステムやインターネットなどのネットワークを介して、コンテンツ配信センタ（不図示）から入手し、コンテンツ格納装置 13 に格納するようにしてよい。いずれにしても、コンテンツデータは暗号化されており、対応するライセンス鍵がなければ復号・再生できない。

以上、本発明の 1 実施形態について説明した。

本実施形態において、コンテンツ格納装置 13 に格納されたコンテンツデータは暗号化されているので、対応するライセンス鍵がなければ復号し再生することができない。したがって、コンテンツ格納装置 13 にコピー防止機能といった特別な機能を設ける必要がなくなるため、コンテンツ格納装置 13 として、一般に市販されている大容量のハードディスク装置などを利用できる。このため、大量のコンテンツデータを格納することが可能となる。

また、コンテンツ格納装置 13 に格納されたコンテンツデータを復号するためには対応するライセンス鍵が必要となるため、このライセンス鍵が鍵格納専用装置 14 に格納されていなければ、当該コンテンツデータを再生することができない。したがって、正当な権利者（対応するライセンス鍵を有する者）のみに、コンテンツデータの再生を許可することができ、コンテンツ著作者などの保護を図ることができる。

さらに、本実施形態では、暗号化されたコンテンツデータの復号を、コンテンツデータの再生を行うオーディオ再生装置18/ビデオ再生装置19で行うようにしている。そして、鍵格納専用装置14は、ライセンス鍵の送信相手がオーディオ再生装置18/ビデオ再生装置1であることを認証した場合に、当該ライセンス鍵を暗号通信を利用してオーディオ再生装置18/ビデオ再生装置19に送るようにしている。このようにすることで、ライセンス鍵が外部に漏れる可能性をより低くすることができ、セキュリティを向上できる。

くわえて、本実施形態において、鍵格納専用装置14は、ライセンス鍵の送信相手がメモリカード30である場合、送信したライセンス鍵を鍵格納専用装置14の記憶内容から消去するようにしている。つまり、鍵格納専用装置14にライセンス鍵のコピー防止機能を設けている。このようにすることで、ライセンス鍵が不正にコピーされる可能性を減らすことができる。

なお、一般に、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば、著しく小さい。このため、鍵格納専用装置14の記憶部をフラッシュメモリ143で構成した場合でも、当該フラッシュメモリ143に多くのライセンス鍵を格納することができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

たとえば、上記の実施形態では、暗号化されたコンテンツデータがたとえばハードディスク装置などの記憶装置でなるコンテンツ格納装置13に格納されている場合を例に取り説明した。しかしながら、本発明はこれに限定されるものではない。暗号化されたコンテンツデータは、D

VDやCDなどの可搬性を有する記憶媒体に格納された形態で提供されるものでもよい。この場合、本実施形態において、コンテンツ格納装置13に代えて前記可搬性を有する記憶媒体から暗号化されたコンテンツデータを読み取る読取装置を設けるようにすればよい。

また、上記の実施形態において、鍵格納専用装置14を装着自在に構成してもよい。たとえば、鍵格納専用装置14として、メモリカード30を用い、カード接続装置20に装着するようにしてもよい。あるいは、本コンテンツ再生装置に、鍵格納専用装置14専用のスロットを設け、このスロットに鍵格納専用装置14を装着するようにしてもよい。上述したように、鍵のデータサイズは、暗号化されたコンテンツデータのデータサイズに比べれば著しく小さいので、多くのライセンス鍵を鍵格納専用装置14に格納することができる。このため、再生するコンテンツを変えるときに鍵格納専用装置14を差し替えなければならないといった事態が頻繁に生じるのを防ぐことができる。したがって、家のなかでコンテンツデータの再生を楽しむような据置型に適したコンテンツ再生装置を提供できる。

さらに、上記の実施形態では、ライセンス鍵を暗号化されたコンテンツデータ毎に用意しているが、本発明はこれに限定されない。たとえば、複数の暗号化されたコンテンツデータを1グループとして、グループ毎に、当該グループに属する暗号化されたコンテンツデータを復号するためのライセンス鍵を用意するようにしてもよい。

以上説明したように、本発明によれば、コンテンツ著作者などの保護を図りつつも、メモリカードの交換なしに、大量のコンテンツデータを再生できるようにすることが可能となる。

## 請求の範囲

1. 暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた計算機能付き鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

2. 請求項1記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、本コンテンツ再生装置に装着自在に構成されていること

を特徴とするコンテンツ再生装置。

3. 請求項 1 記載のコンテンツ再生装置であって、

暗号化されたコンテンツデータを復号するための鍵が記憶された計算機能付き記憶媒体を接続するための接続手段をさらに有し、

前記計算機能付き鍵格納手段は、

前記接続手段に接続された前記計算機能付き記憶媒体より、暗号通信を利用して送信された鍵を格納すること

を特徴とするコンテンツ再生装置。

4. 請求項 3 記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、

前記認証手段により、前記接続手段に接続された前記計算機能付き記憶媒体が通信相手として認証された場合に、暗号通信を利用して、自身が保持している鍵を読み出して前記計算機能付き記憶媒体に送信するとともに、送信した鍵を記憶内容から消去すること

を特徴とするコンテンツ再生装置。

5. 暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、再生対象の暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記計算機能付き鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

前記再生手段は、

前記コンテンツ読取手段を介して前記記憶媒体から読み出された、再生対象の暗号化されたコンテンツデータを、前記計算機能付き鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生することを特徴とするコンテンツ再生装置。

6. 請求項 5 記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、本コンテンツ再生装置に装着自在に構成されていること  
を特徴とするコンテンツ再生装置。

7. 請求項 5 記載のコンテンツ再生装置であって、

暗号化されたコンテンツデータを復号するための鍵が記憶された計算機能付き記憶媒体を接続するための接続手段をさらに有し、

前記計算機能付き鍵格納手段は、

前記接続手段に接続された前記計算機能付き記憶媒体より、暗号通信を利用して送信された鍵を格納すること  
を特徴とするコンテンツ再生装置。

8. 請求項 7 記載のコンテンツ再生装置であって、

前記計算機能付き鍵格納手段は、

前記認証手段により、前記接続手段に接続された前記計算機能付き記憶媒体が通信相手として認証された場合に、暗号通信を利用して、自身が保持している鍵を読み出して前記計算機能付き記憶媒体に送信するとともに、送信した鍵を記憶内容から消去すること  
を特徴とするコンテンツ再生装置。

9. 暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、  
暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納装置を接続するための接続手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記接続手段によって接続された前記計算機能付き鍵格納装置より、暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

10. 暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータが記憶された可搬性を有する記憶媒体から、再生対象の暗号化されたコンテンツデータを読み取るコンテンツ読取手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する、計算機能付き鍵格納装置を接続するための接続手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記再生手段は、

前記コンテンツ読み取り手段を介して前記記憶媒体から読み出された、再生対象の暗号化されたコンテンツデータを、前記接続手段によって接続された前記計算機能付き鍵格納装置より、暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

1 1 . 暗号化されたコンテンツデータを復号して再生するコンテンツ再生装置に装着されて用いられる計算機能付き鍵格納装置であって、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータを復号するための鍵を格納する鍵格納手段と、通信相手を認証する認証手段と、

前記認証手段により前記コンテンツ再生装置が通信相手として認証された場合に、再生対象の暗号化されたコンテンツデータに対応する鍵を前記鍵格納手段から読み出し、暗号通信を利用して前記コンテンツ再生装置に送信する通信手段と、を有すること

を特徴とする計算機能付き鍵格納装置。

1 2 . 暗号化されたコンテンツデータを再生するコンテンツ再生装置であって、

暗号化されたコンテンツデータを格納するコンテンツ格納手段と、

暗号化されたコンテンツデータもしくは当該データのグループ毎に用意されたコンテンツデータの復号するための鍵を格納する、前記コンテンツ格納手段とは別個に設けられた復号鍵を記録する鍵格納手段と、

暗号化されたコンテンツデータを復号して再生する再生手段と、を備え、

前記復号鍵を記録する鍵格納手段は、

通信相手を認証する認証手段を有し、前記認証手段により前記再生手段が通信相手として認証された場合に、暗号通信を利用して、前記再生手段に、再生対象の暗号化されたコンテンツデータに対応する鍵を送信し、

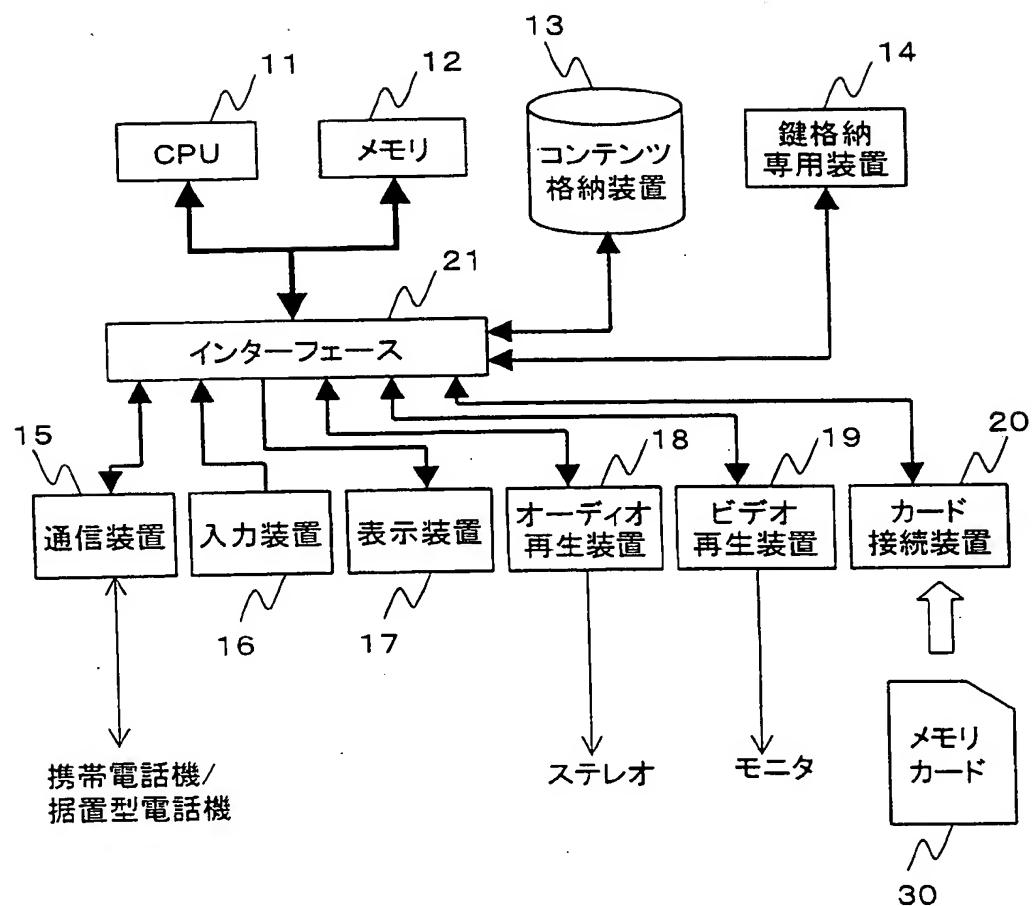
前記再生手段は、

前記コンテンツ格納手段から読み出された、再生対象の暗号化されたコンテンツデータを、前記復号鍵を記録する鍵格納手段より暗号通信を利用して送信された鍵を用いて復号し、再生すること

を特徴とするコンテンツ再生装置。

図1

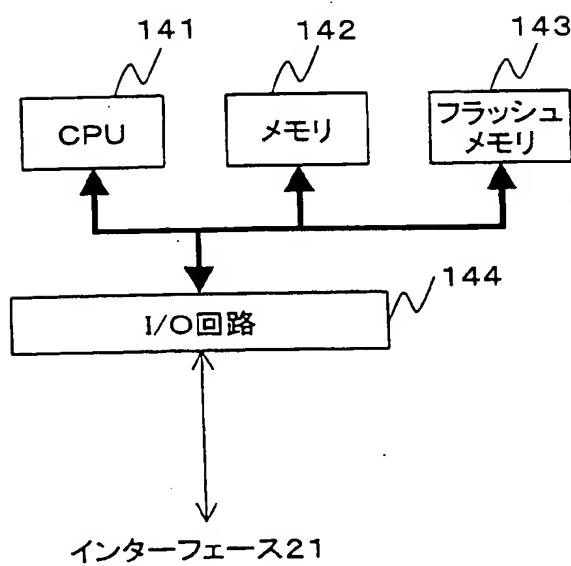
## コンテンツ再生装置



2/10

図2

## 鍵格納専用装置14



3/10

図3

## オーディオ再生装置18

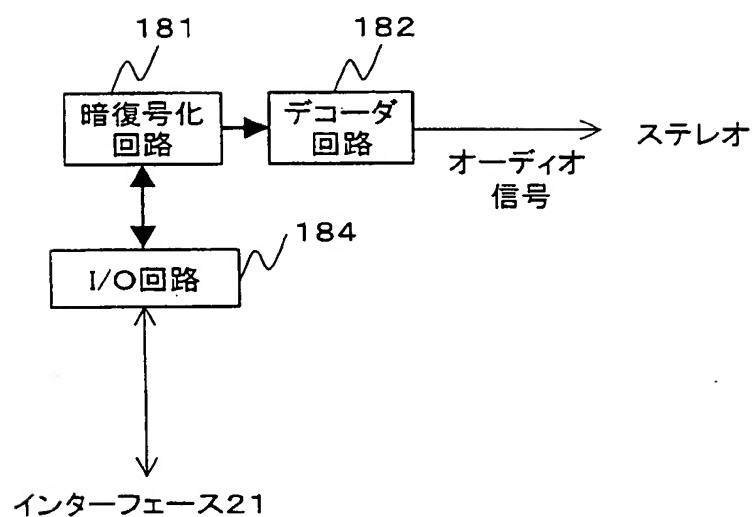
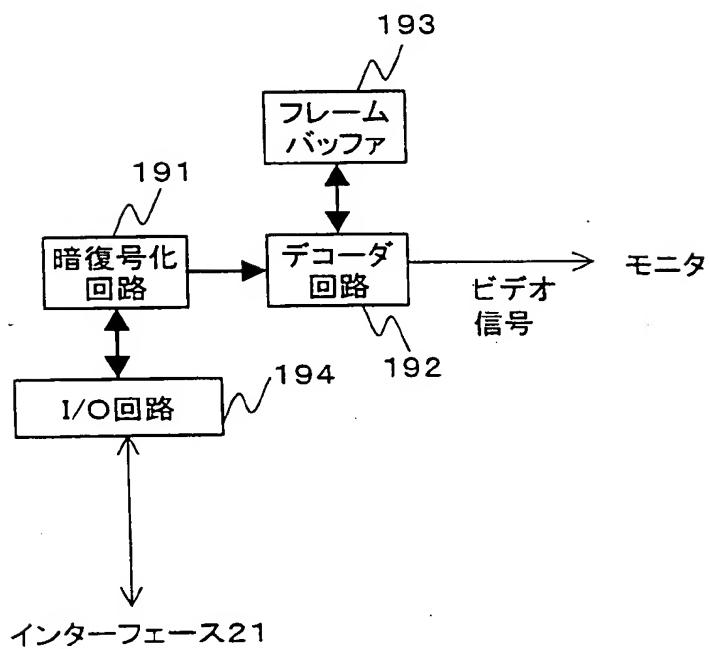


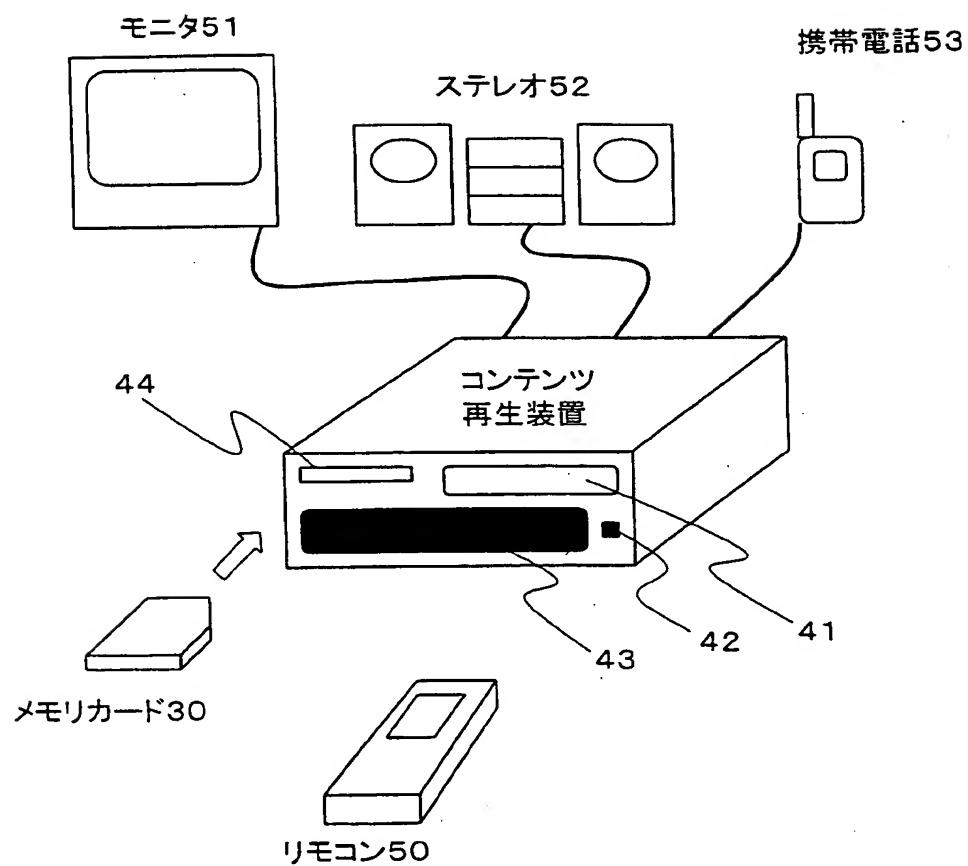
図4

ビデオ再生装置19



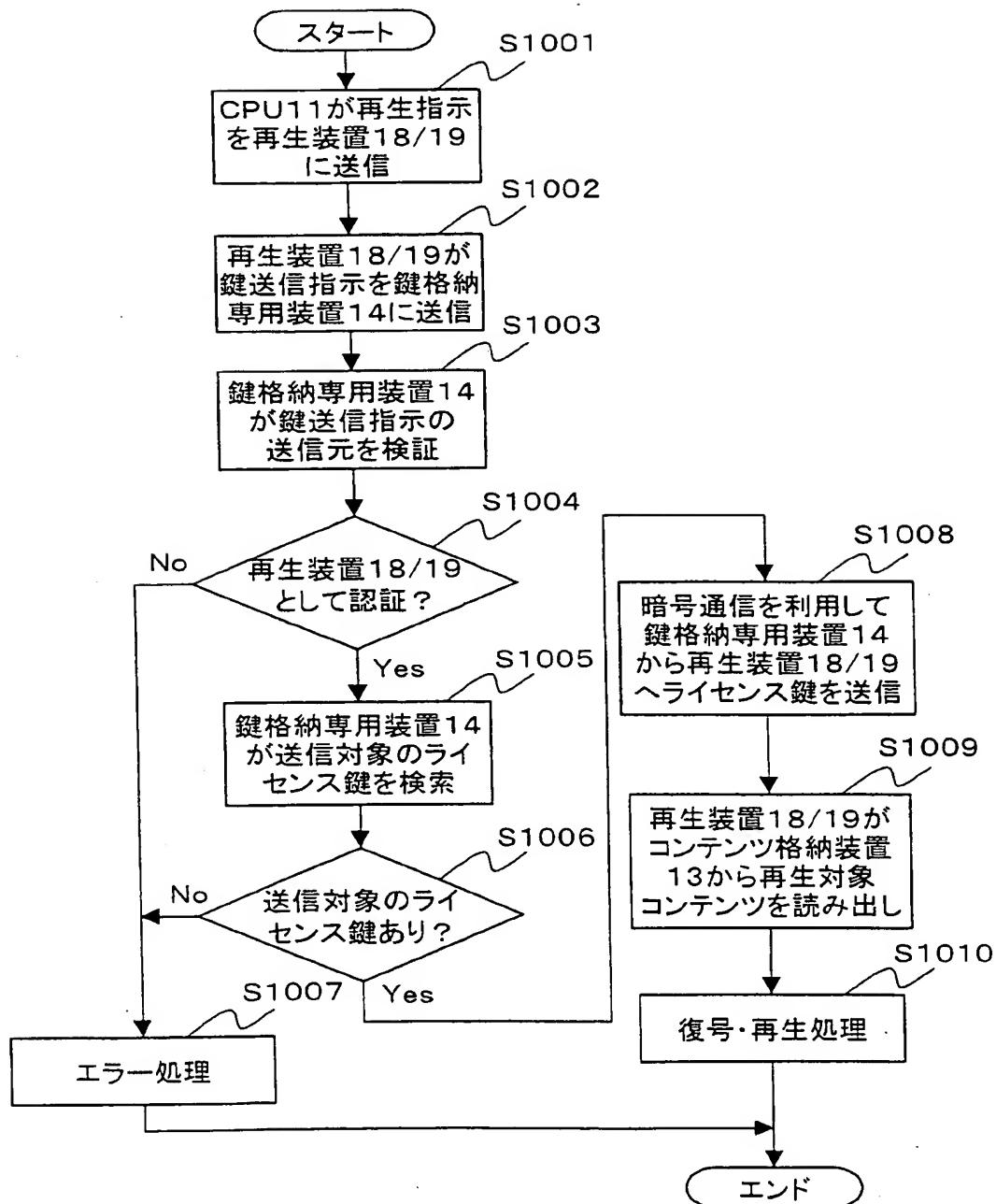
5/10

図5



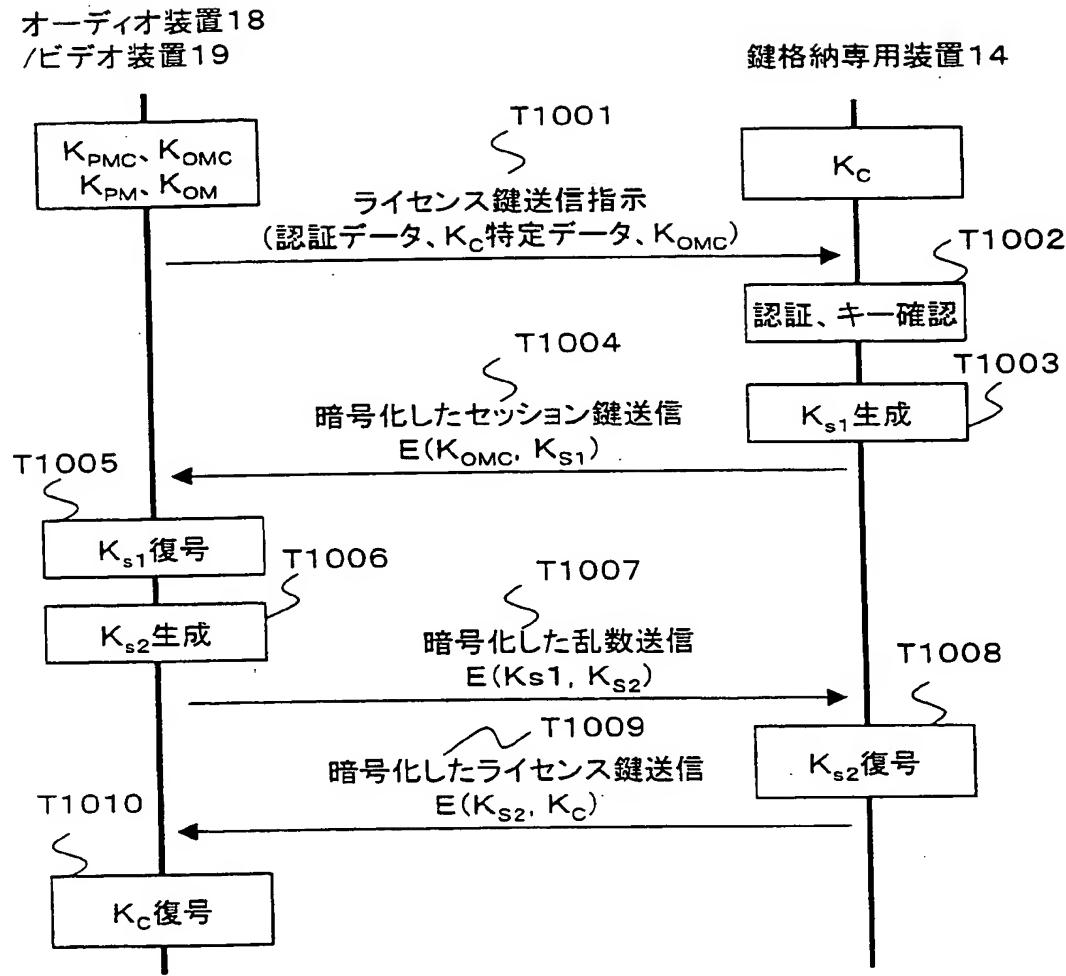
6/10

図6



7/10

図7



$K_{PMC}$ : メディアクラス秘密鍵  
 $K_{OMC}$ : メディアクラス公開鍵  
 $K_{s2}$ : 乱数

$K_c$ : ライセンス鍵  
 $K_{s1}$ : セッション鍵

8/10

図8

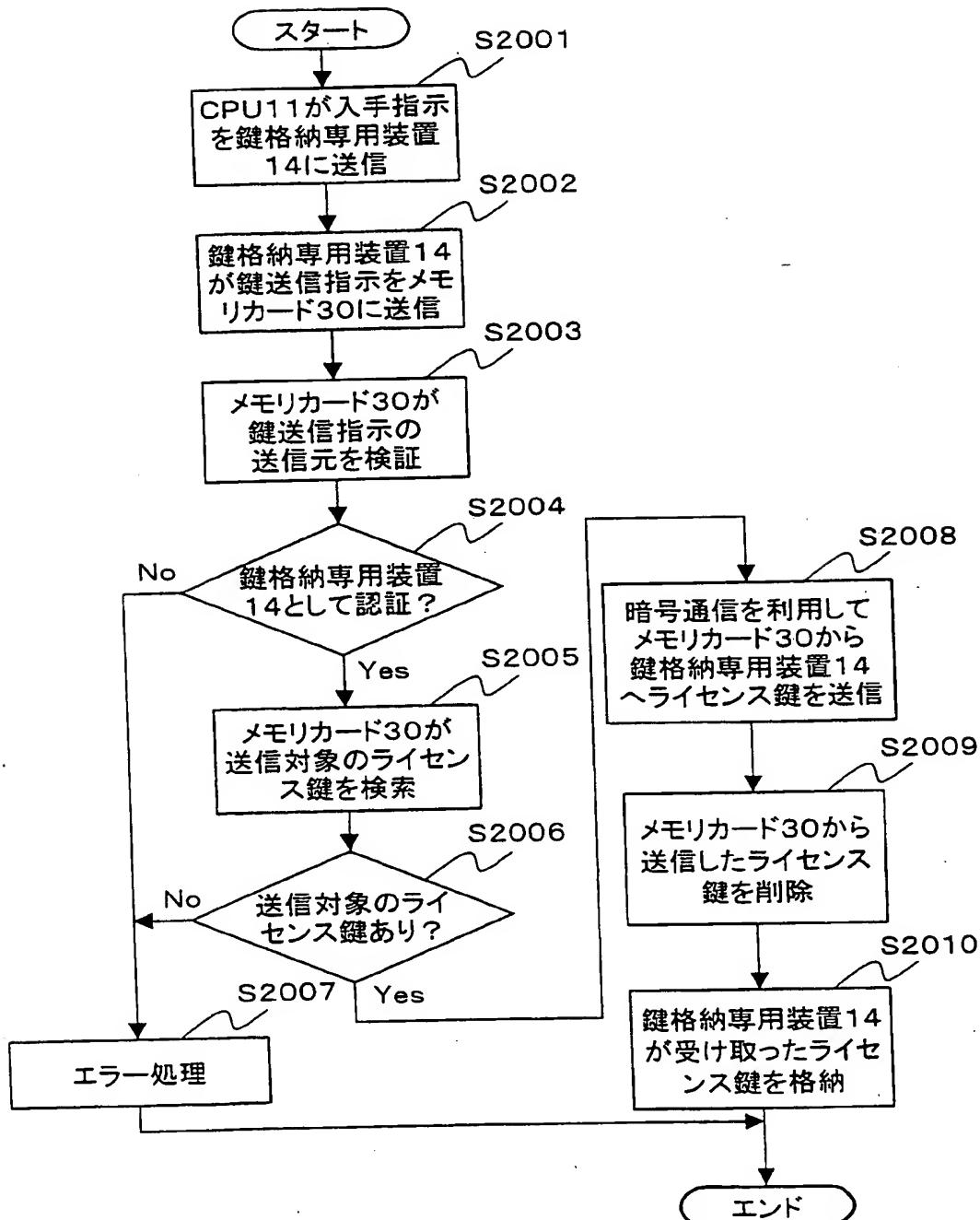
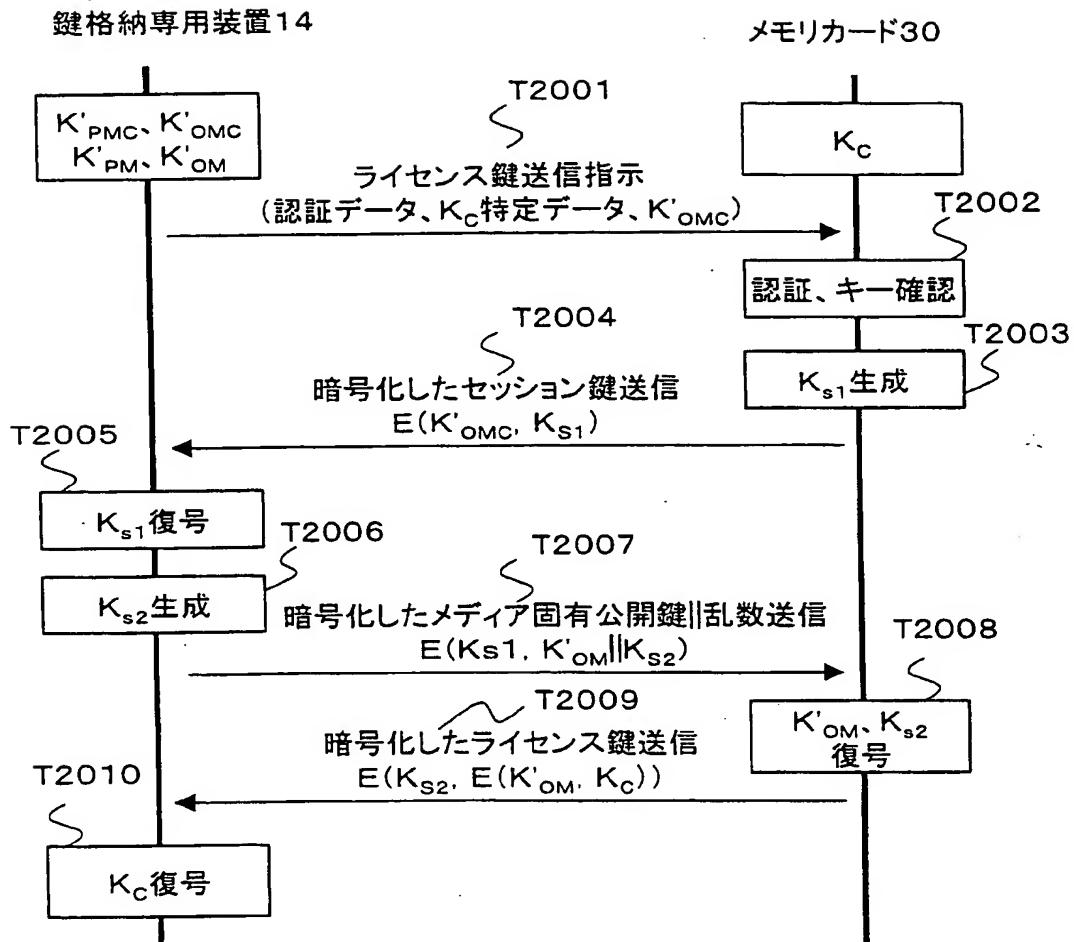


図9

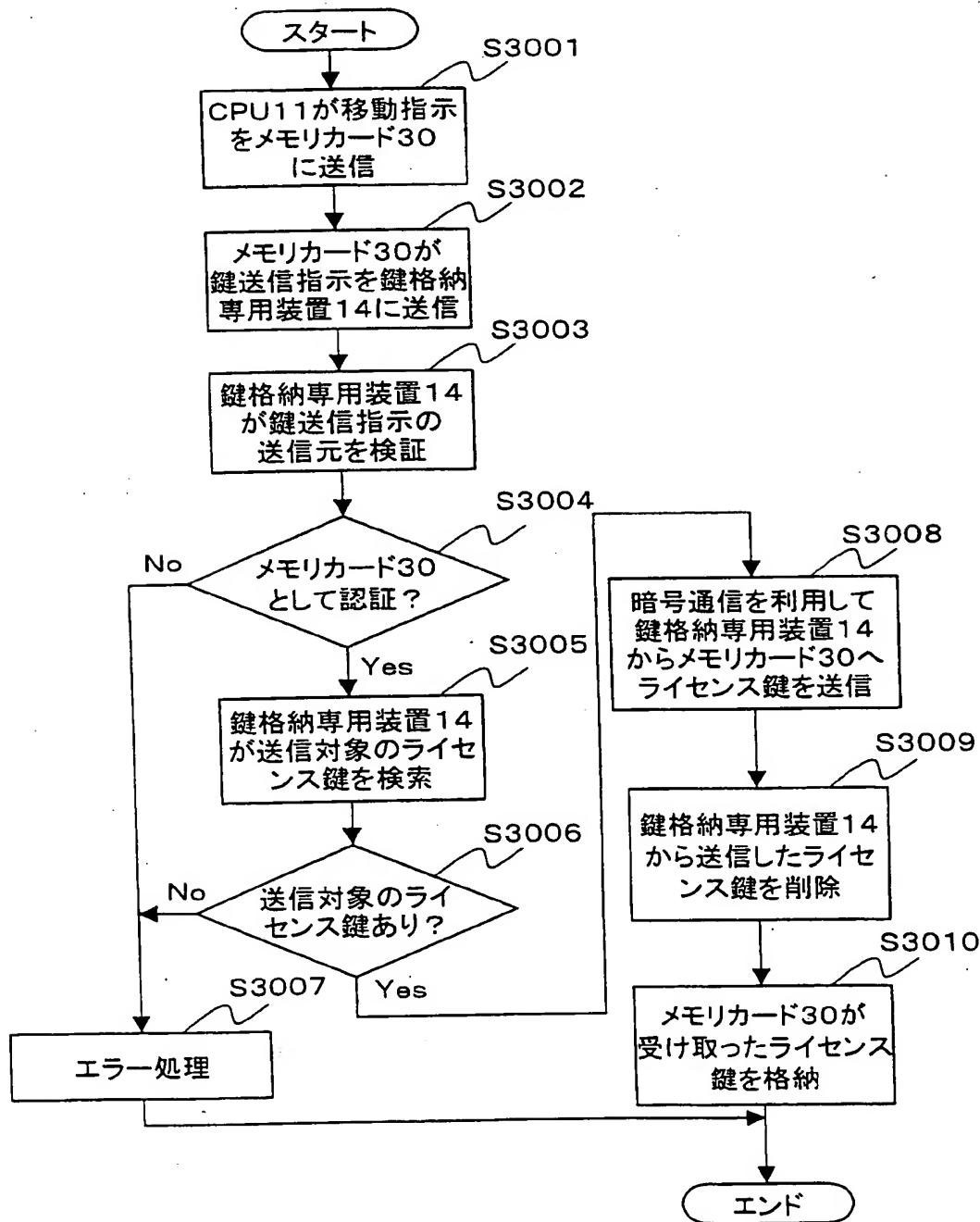


$K'_{PMC}$ : メディアクラス秘密鍵  
 $K'_{OMC}$ : メディアクラス公開鍵  
 $K'_{PM}$ : メディア固有秘密鍵  
 $K'_{OM}$ : メディア固有公開鍵  
 $K_{s2}$ : 亂数

$K_c$ : ライセンス鍵  
 $K_{s1}$ : セッション鍵

10/10

図10



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02003

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L9/08, H04L9/10, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> H04L9/08, H04L9/10, H04L9/32Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001  
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Kiyoshi YAMANAKA et al., "Multimedia on demande Service ni okeru Joho Hogo System", NTT R & D, Vol.44, No.9, 10 September, 1995 (10.09.95) pp.813-818	1-7, 9-12 8
Y	JP, 9-307543, A (Matsushita Electric Ind. Co., Ltd.), 28 November, 1997 (28.11.97), Par. Nos. [0018] to [0019], [0022], [0024] to [0025]; Figs. 1 to 8 (Family: none)	8
A	"Kogata Memory Card de Ongaku Chosakuken wo mamoru", Nikkei Elecrtonics, 1999 3-22, No.739, 22 March, 1999 (22.03.99) pp.49-53	1-12
A	JP, 4-102185, A (NTT Data Tsushin K.K.), 03 April, 1992 (03.04.92), Full text; Figs. 1 to 2 (Family: none)	1-12

 Further documents are listed in the continuation of Box C. See patent family annex.

- \* Special categories of cited documents:
- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search  
08 June, 2001 (08.06.01)Date of mailing of the international search report  
19 June, 2001 (19.06.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP01/02003

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 10-40172, A (Toshiba Corporation), 13 February, 1998 (13.02.98), Full text; Figs. 1 to 4 (Family: none)	1-12

## A. 発明の属する分野の分類（国際特許分類（IPC））

Int. C1' H04L9/08, H04L9/10, H04L9/32

## B. 調査を行った分野

## 調査を行った最小限資料（国際特許分類（IPC））

Int. C1' H04L9/08, H04L9/10, H04L9/32

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

## 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	中山喜義、高嶋洋一、小柳津育郎；“マルチメディアオンデマンドサービスにおける情報保護システム” NTT R&D, Vol. 44, No. 9, 10. 9月. 1995 (10. 09. 95) pp. 813-818	1-7, 9-12
Y	pp. 813-818	8
Y	J P, 9-307543, A (松下電器産業株式会社) 28. 11月. 1997 (28. 11. 97) 第【0018】-【0019】段落、第【0022】段落、	8

 C欄の続きにも文献が列举されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

## 国際調査を完了した日

08. 06, 01

## 国際調査報告の発送日

19.06.01

## 国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

## 特許庁審査官（権限のある職員）

青木 重徳

印 5M 4229

電話番号 03-3581-1101 内線 3597

C (続き) 関連すると認められる文献	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
引用文献の カテゴリー*		
	第【0024】-【0025】段落、図1-8 (ファミリーなし)	
A	“小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス、1999 3-22, No. 739, 22. 3月. 1999 (22. 03. 99) p. 49-53	1-12
A	JP, 4-102185, A (エヌ・ティ・ティ・データ通信株式会社) 3. 4月. 1992 (03. 04. 92) 全文、第1-2図 (ファミリーなし)	1-12
A	JP, 10-40172, A (株式会社東芝) 13. 2月. 1998 (13. 02. 98) 全文、図1-4 (ファミリーなし)	1-12